JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Detecting Network Events

CYBER INCIDENT RESPONSE

Detecting Network Events

- Cybersecurity analysts should be able to determine an incident based on events
- Analysis of logs and other data are key to understanding if an event will become an incident
- Types of Network Events:
  - Beaconing
  - Unusual bandwidth consumption
  - Link and connection failures
  - Unexpected traffic

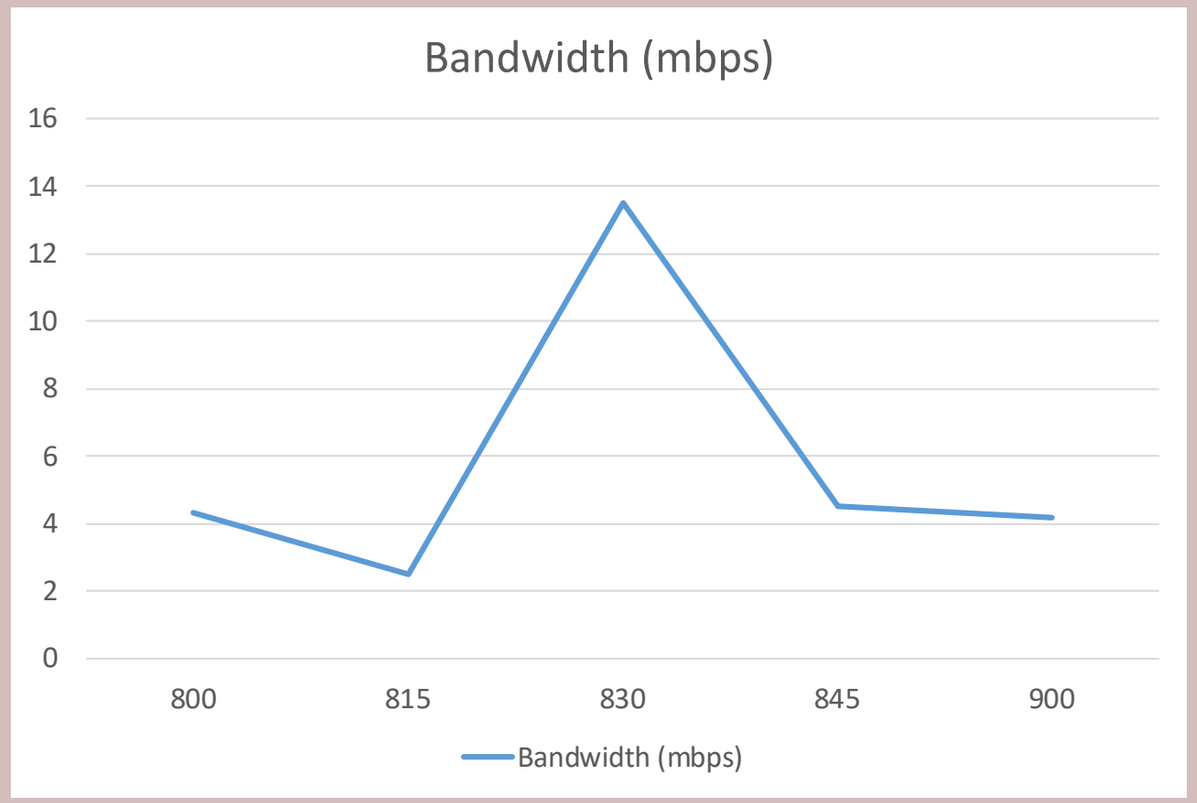
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Beaconing

- Beaconing or a heartbeat sends a signal to a Command and Control system due to a botnet or malware infection
- Usually sent over HTTP or HTTPS
- Can be difficult to detect
- Generally occurs at a certain frequency or pattern

Unusual Bandwidth Consumption

- Unusual bandwidth consumption could cause service issues or can be a sign of larger trouble

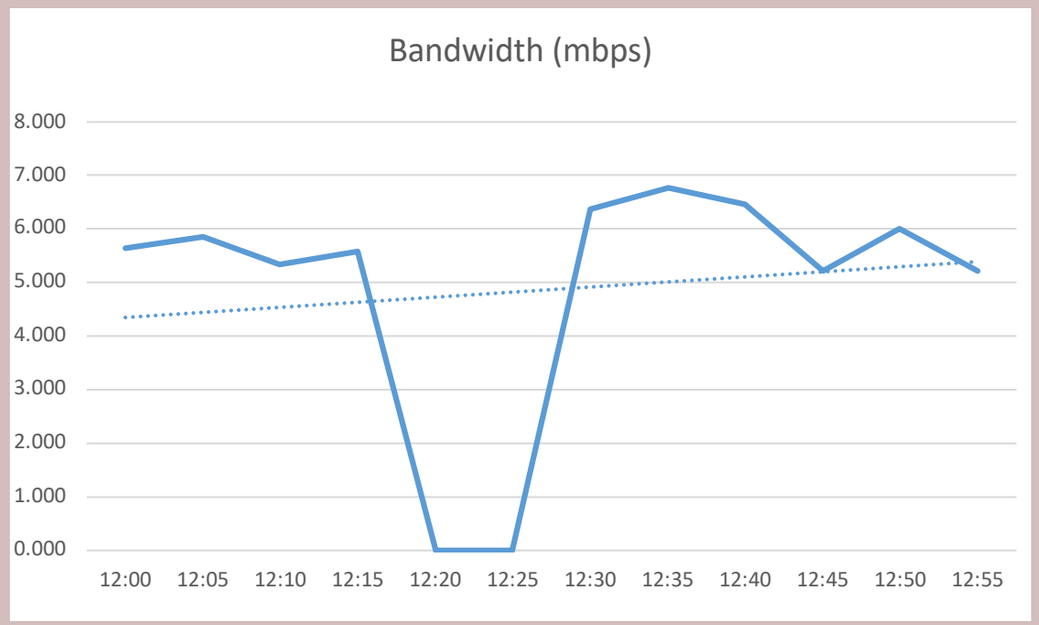


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Link and Connection Failures

- Generally occur due to a hardware, firmware, or software issues

- Could be as simple as a bad module, broken cable, or unplugged connector



Unexpected Traffic

- Detected by IDS/IPS, traffic monitoring systems, or by manual observation
- Understanding your baseline is important
- Not all unexpected traffic is malicious, but it should be investigated/understood
- Could be unusual based on type of traffic, end point location, or amount

Detecting Unexpected Traffic

- Baselines or Anomaly-based
  - Monitoring system alarm based on traffic that is outside the normal baseline
- Heuristics or Behavior-based
  - Uses signatures and defined rules to detect
- Protocol Analysis
  - Seeks to detect protocols where they aren't expected, like VPNs or IPv6 tunnels